

## WHAT IS CLAIMED IS:

1. A method for e-commerce with a check, the method comprising:  
providing a purchaser with an encoded personal identification number (PIN);  
receiving the encoded PIN in response to an offer of payment by the purchaser to a  
5 merchant with a check, by a bank associated with the check, wherein the bank is  
to decode the encoded PIN;  
decoding the encoded PIN; and  
comparing the decoded PIN with information associated with the purchaser to  
authenticate the purchaser and to verify that sufficient funds are available to the  
10 purchaser for the transaction.
2. The method of claim 1, wherein providing the purchaser with the encoded PIN comprises  
providing the purchaser with software to generate the encoded PIN, wherein generating  
the encoded PIN comprises encrypting a PIN.
3. The method of claim 1, wherein providing the purchaser with the encoded PIN comprises  
15 interacting with the purchaser to generate the encoded PIN prior to the transaction.
4. The method of claim 1, wherein receiving the encoded PIN comprises receiving the  
encoded PIN, forwarded by the merchant to the bank, in an encrypted form such that the  
merchant is a conduit through which the purchaser transmits to the encoded PIN to the  
bank.
- 20 5. The method of claim 1, wherein receiving the encoded PIN comprises receiving the  
transaction information with the encoded PIN, wherein the transaction information  
comprises a routing number, a bank account number, a check number, and an amount  
associated with the transaction.
6. The method of claim 1, wherein decoding the encoded PIN comprises decrypting the  
25 encoded PIN.
7. The method of claim 6, wherein decoding the encoded PIN further comprises decoding  
data embedded in the encoded PIN based upon a unique transaction number associated  
with the purchaser.

8. The method of claim 6, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN based upon an amount associated with the transaction.
9. The method of claim 6, wherein decoding the encoded PIN further comprises decoding data embedded in the encoded PIN based upon a date associated with the transaction.
- 5 10. The method of claim 1, wherein comparing the decoded PIN comprises comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction.

11. An apparatus for e-commerce with a check, the apparatus comprising:  
a PIN module to provide a purchaser with an encoded personal identification number (PIN);  
a purchaser database to maintain information associated with the purchaser and an  
5 account associated with the purchaser; and  
a PIN processor to receive the encoded PIN in response to an offer of payment by the purchaser to a merchant with a check, decode the encoded PIN, and compare the decoded PIN with the information associated with the purchaser to authenticate the purchaser and to verify that sufficient funds are available to the purchaser for  
10 the transaction.
12. The apparatus of claim 11, wherein the PIN module comprises a client-side software application configured to generate the encoded PIN, the client-side software being configured to independently determine a unique transaction identification that authenticates the purchaser for the transaction to a bank associated with the account.
- 15 13. The apparatus of claim 11, wherein the PIN module comprises a software application configured to interact with a purchaser to encrypt a password to generate the encoded PIN.
14. The apparatus of claim 11, wherein the PIN processor is configured to receive the encoded PIN from the merchant, wherein the encoded PIN is designed to prevent the  
20 merchant from accessing identification information of the encoded PIN.
15. The apparatus of claim 11, wherein the PIN processor comprises a PIN decrypter to decrypt the encoded PIN.
16. The apparatus of claim 15, wherein the PIN processor further comprises a PIN decoder to decode the decrypted, encoded PIN.
- 25 17. The apparatus of claim 11, wherein the PIN processor comprises a comparator to compare the transaction amount with funds available to the purchaser for the transaction.

18. The apparatus of claim 17, wherein the comparator is configured to compare a password embedded in the decoded PIN against a password received from the purchaser for the transaction.

19. A machine-accessible medium containing instructions, which when executed by a machine, cause said machine to perform operations, comprising:  
providing a purchaser with an encoded personal identification number (PIN);  
receiving the encoded PIN in response to an offer of payment by the purchaser to a  
5 merchant with a check, by a bank associated with the check, wherein the bank is  
to decode the encoded PIN;  
decoding the encoded PIN; and  
comparing the decoded PIN with information associated with the purchaser to  
authenticate the purchaser and to verify that sufficient funds are available to the  
10 purchaser for the transaction.
20. The machine-accessible medium of claim 19, wherein providing the purchaser with the encoded PIN comprises providing the purchaser with software to generate the encoded PIN.
21. The machine-accessible medium of claim 19, wherein providing the purchaser with the  
15 encoded PIN comprises interacting with the purchaser to encrypt a PIN to generate the encoded PIN prior to the transaction.
22. The machine-accessible medium of claim 19, wherein decoding the encoded PIN comprises decrypting the encoded PIN.
23. The machine-accessible medium of claim 22, wherein decoding the encoded PIN further  
20 comprises decoding data embedded in the encoded PIN.
24. The machine-accessible medium of claim 19, wherein comparing the decoded PIN comprises comparing a password embedded in the decoded PIN against a password received from the purchaser for the transaction.